16869N-103900

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月２８日

出願番号
Application Number: 特願２００３－３６７１５２

[ST. 10/C]: [ＪＰ２００３－３６７１５２]

出願人
Applicant(s): 株式会社日立製作所

２００３年１２月 ４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３１００５１６

【書類名】　特許願
【整理番号】　NT03P0753
【提出日】　平成15年10月28日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F　3/06
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　白銀　哲也
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　100068504
　【弁理士】
　【氏名又は名称】　小川　勝男
　【電話番号】　03-3661-0071
【選任した代理人】
　【識別番号】　100086656
　【弁理士】
　【氏名又は名称】　田中　恭助
　【電話番号】　03-3661-0071
【選任した代理人】
　【識別番号】　100094352
　【弁理士】
　【氏名又は名称】　佐々木　孝
　【電話番号】　03-3661-0071
【手数料の表示】
　【予納台帳番号】　081423
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
ＩＰネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、
該コマンドによって処理される対象となるデータを記憶する記憶装置と、
該ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、
該ホストコンピュータから送信されるログイン要求に関して、該ログイン要求のフレームに該ホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定する第一判定手段と、
該第一判定手段による判定の結果、該ログイン要求フレームに、意図する第二の情報が含まれていない場合には、該ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求する手段と、
該要求手段からの要求に対する応答として、該ホストコンピュータから獲得した第一の情報に関して、該アクセス管理テーブルを参照して判定する第二判定手段と、
該第二判定手段による判定の結果に応じて、該ログイン要求の許可を行うことを特徴とするストレージ装置。
【請求項２】
該記憶装置は、iSCSIプロトコルによりアクセスさせることを特徴とする請求項１記載のストレージ装置。
【請求項３】
前記アクセス管理テーブルに格納される第一の情報は、ホストコンピュータが接続されるＩＰネットワークのインタフェースのＭＡＣアドレスである請求項１又は２記載のストレージ装置。
【請求項４】
該ストレージ装置は、ＩＰネットワークに接続される装置を監視するためのＳＮＭＰマネージャを有し、該ＳＮＭＰマネージャは、該ホストコンピュータから第一の情報を送信するように要求するフレームを、該ホストコンピュータに関係するインタフェースのＭＩＢを要求するＳＮＭＰリクエストとして送信することを特徴とする請求項１乃至３のいずれか記載のストレージ装置。
【請求項５】
該ストレージ装置は更に、前記アクセス管理テーブルの内容を変更するための入出力を行うコンソールを備えることを特徴とする請求項１乃至３のいずれかに記載のストレージ装置。
【請求項６】
前記第二の判定手段による判定で、前記アクセス管理テーブルにホストコンピュータを識別する第一の情報が格納されていないと判定した場合に、該ログイン要求の内容をログとして前記メモリに格納する請求項１乃至３のいずれかに記載のストレージ装置。
【請求項７】
前記第二の判定手段による判定で、該アクセス管理テーブルに該ホストコンピュータを識別する第一の情報が格納されていると判定した場合、該ログイン要求フレームのソースＩＰアドレスを、ホストコンピュータを識別する前記情報と関連付けて該アクセス管理テーブルに格納する請求項３記載のストレージ装置。
【請求項８】
該アクセス管理テーブルには、ＭＡＣアドレスと、該ＭＡＣアドレスのＩＰネットワークのインタフェースを持つホストコンピュータがアクセス許可された論理装置（ＬＵ）の識別符号が登録されており、
該ホストコンピュータから送信されたコマンドの処理に関して、予め許可された論理装置へのアクセスか否かの判定を行ない、許可された論理装置に対して該コマンドの処理を行なうことを特徴とする請求項３記載のストレージ装置。

【請求項９】
該アクセス管理テーブルには、該ＭＡＣアドレスに関連付けた該ＭＡＣアドレスのＩＰネットワークインタフェースを持つホストコンピュータのＩＰアドレスが格納される請求項３又は８記載ストレージ装置。
【請求項１０】
外部の装置からネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理するアクセス制御の管理方法において、
外部から送信されるログイン要求のフレームをストレージ装置で受信するステップと、
受信した該フレームに該外部の装置を特定する第二の情報が含まれているかを判定する第一の判定ステップと、
第一の判定の結果、該フレームに該第二の情報が含まれていない場合、該外部の装置に対してそれを特定する第一の情報の取得を要求するステップと、
取得された該第一の情報に関してチェックを行い、アクセス許可をすべきかを判定する第二の判定ステップと、
該第二の判定の結果、許可された場合に該外部の装置からストレージ装置に対するアクセス要求を許可するステップと、
を有することを特徴とするアクセス制御管理方法。
【請求項１１】
前記第一の情報としてＭＡＣアドレスを使用し、前記第二の情報としてＩＰアドレスを使用する請求項１０記載のアクセス制御管理方法。
【請求項１２】
該ストレージ装置へのアクセスが許可された外部装置を特定する第一の情報を登録するテーブルをメモリに予め用意するステップを有し、
前記第二の判定ステップは、外部装置から取得された第一の情報に関して、該テーブルを参照することにより判定を行うことを特徴とする請求項９記載のアクセス制御管理方法。
【請求項１３】
前記第一の判定ステップによる判定の結果、又は第二の判定ステップによる判定の結果、不適合の場合、受信されたログイン要求のフレームに関する情報をログとしてメモリに格納するステップを有することを特徴とする請求項９記載のアクセス制御管理方法。
【請求項１４】
前記第一の情報の取得を要求ステップにおいて、ＩＰネットワークに接続される装置を監視するためのＳＮＭＰマネージャにより該外部の装置から第一の情報を送信するように要求することを特徴とする請求項９記載のアクセス制御管理方法。
【請求項１５】
前記第一の情報の取得を要求ステップにおいて、iSCSIのTEXT Mode negotiationによるプロトコルを用いて該外部の装置からＭＡＣアドレスを得ることを要求することを特徴とする請求項９記載のアクセス制御管理方法。
【請求項１６】
該ストレージ装置に複数の論理装置（ＬＵ）を定義するステップと、
ＭＡＣアドレスと、ＭＡＣアドレスのＩＰネットワークのインタフェースを持つ外部の装置がアクセス許可されたＬＵの識別符号が登録されたアクセス管理テーブルを用意するステップと、
前記第二の判定ステップの後に、外部の装置から送信されたコマンドの処理に関して、該テーブルを参照して予め登録されたＬＵに対するアクセスか否かを判定する第三の判定ステップと、を有し、
該第三の判定の結果、許可されたＬＵに対して該コマンドの処理を行なうことを特徴とする請求項１２記載のアクセス制御管理方法。
【請求項１７】
ネットワークに接続された第一の装置から第二の装置へのアクセスに関する許可を管理する方法において、

第一の装置から第二の装置に対するアクセスが同一のネットワーク間で行われるか否かを該第一の装置から送信される第二の情報を用いてチェックする第一のチェックモードと、
該第一のチェックモードにおいて、同一のネットワーク間の通信でないと判定された場合、送信元となる該第一の装置から所定の第一の情報を獲得するステップと、
獲得された該第一の情報を用いて該第二の装置へのアクセスの許可の可否をチェックする第二のチェックモードと、
該第二のチェックモードにおいて許可された場合に、該第一の装置から該第二の装置へ送信されるコマンドの処理を行うことを特徴とするアクセスの管理方法。
【請求項１８】
前記第一の装置はホストコンピュータであり、第二の装置は複数の論理装置が規定され、iSCSIプロトコルによりコマンド処理されるストレージ装置であり、該第一の情報はＭＡＣアドレスであり、該第二の情報は該第一の装置から送信されたフレームに含まれるＩＰアドレスである請求項１７記載のアクセスの管理方法。
【請求項１９】
iSCSI層、ＴＣＰ層、ＩＰ層、データリンク層を有するストレージ装置をＩＰネットワークに接続するステップを更に有すること特徴とする請求項１０又は１８記載のアクセスの管理方法。
【請求項２０】
iSCSIイニシエタを有する第一の装置と、iSCSIターゲットを有する第二の装置との間でＩＰネットワークを介して通信を行って、コマンドの処理を行う方法において、
第一の装置から送信されるログイン要求のフレームを第二の装置で受信し、
受信した該フレームに該第一の装置を特定する所定の情報が含まれているかをチェックし、
該チェックの結果、該フレームに該所定の情報が含まれていない場合、該第二の装置から該第一の装置に対して該第一の装置を特定する他の所定の情報の取得を要求し、
該第一の装置から第二の装置へ送信された他の所定の情報に関して、該第一の装置からのアクセスを許可すべきか否かをチェックし、
該チェックの結果、許可された場合に該第一の装置から送信されるコマンドを該第二の装置のiSCSI上で処理することを特徴とするコマンドの処理方法。
【請求項２１】
該第一の装置に備えられるＳＮＭＰエージェントと、該第二の装置に備えられるＳＮＭＰマネージャとの間の通信により他の所定の情報であるＭＡＣアドレスの取得が行われることを特徴とする請求項２０記載のコマンドの処理方法。
【請求項２２】
ＩＰネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、
該コマンドによって処理される対象となるデータを記憶する記憶装置と、
該ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、
該ホストコンピュータからの要求を処理する処理装置とを有し、
該処理装置は、
該ホストコンピュータから送信されるログイン要求に関して、該ログイン要求のフレームに該ホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定し（第一の判定）、該第一の判定の結果、該ログイン要求フレームに、意図する第二の情報が含まれていない場合には、該ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求し、該要求手段からの要求に対する応答として、該ホストコンピュータから獲得した第一の情報に関して該アクセス管理テーブルを参照して判定し（第二の判定）、該第二の判定の結果に応じて、該ログイン要求の許可を行うことを特徴とするストレージ装置。

【書類名】明細書
【発明の名称】ストレージ装置及びそのアクセス管理方法
【技術分野】
【０００１】
本発明は、ストレージ装置及びそのアクセス管理方法に係り、特にホストコンピュータ（以下単にホストと言う）からiSCSIプロトコルによってストレージ装置内のデータをアクセスするストレージシステムにおけるセキュリティの管理に関する。
【背景技術】
【０００２】
単体又は複数のハードディスクドライブの集合体、若しくは専用の制御部で複数のハードディスクドライブを制御するディスクアレイ装置等から成るストレージ装置（記憶装置システム）を、インタフェースを介してホストと接続して、ホストからアクセスするストレージシステムが実用化されている。通常、ストレージ装置は、１つ又は複数のボリュームと称する論理装置（Logical Unit:ＬＵ）を持ち、論理装置にはＩＤ番号又は論理装置番号（ＬＵＮ）が割当てられる。
【０００３】
ストレージ装置とホストを接続するインタフェース技術としては、SCSI（Small Computer Systems Interface）やファイバチャネル(FC)が用いられる。
SCSIインタフェースは安価であり、クライアント/サーバ型を基本とする比較的近距離接続用のインタフェースとして利用されている。SCSIにおいて、クライアントはコマンドを発行する能動的な役割を持ち、イニシエタと呼ばれる。またサーバは、クライアントの要求に従う受動的な役割を持ち、ターゲットと呼ばれる。論理装置に処理を指示するコマンドは、イニシエタから発行されるCommand Descriptor Block（CDB)に含まれる。
【０００４】
このようなストレージシステムにおいて、ストレージ装置内の論理装置(ＬＵ)に対する不正なアクセスを防止するためのセキュリティを実現する技術としては、例えば、特開平１０－３３３８３９公報（特許文献１）或いは特開２００１－２６５６５５公報（特許文献２）に開示されている。
【０００５】
前者は、ＬＵ毎に予めアクセス許可したホストを示すWWN(World Wide Name)との関係をストレージ装置内のテーブルに記憶しておき、ホストからのログインフレームに格納されたＷＷＮとテーブルの内容とを照合するすることによってホストの識別を行い、ストレージ装置内のＬＵへのアクセス可否の判断を行なう。
【０００６】
後者は、ホストのＷＷＮとポートＩＤの関係をテーブルに記憶し、ＷＷＮが格納されていないフレーム（たとえばＣＤＢが格納されたフレーム）について、ポートＩＤから対応するＷＷＮを参照してＬＵのアクセス可否の判断を行なう。
なお以下、ストレージ装置内の特定ＬＵに対するホストからのアクセス可否を制御する方法を、便宜上「ＬＵＮセキュリティ」と呼ぶことにする。
【０００７】
ところで、最近、ネットワークプロトコルであるＴＣＰ／ＩＰ上で、上位プロトコルとしてSCSI処理を実現するためのプロトコル技術であるiSCSI（internet ＳＣＳＩ）が注目されている。iSCSIはＩＰネットワーク上で用いられるプロトコルとして、IETF（The Internet Engineering Task Force）で規格化されたものである。
【０００８】
【特許文献１】特開平１０－３３３８３９公報
【０００９】
【特許文献２】特開２００１－２６５６５５公報
【発明の開示】
【発明が解決しようとする課題】

【００１０】
ＩＰネットワークはファイバチャネルよりも安価であり、より多くのユーザからストレージ装置内のＬＵを利用する形態が取り得ると考えられる。しかし、誤操作や悪意のある攻撃によってＬＵのデータが破壊されてしまった場合に影響を及ぼす範囲も広くなる。このため、ＩＰネットワーク上でiSCSIを用いたストレージ装置内のＬＵに対するアクセスにおいてもＬＵＮセキュリティを保証することが重要である。
【００１１】
ＬＵＮセキュリティのチェックのために、ＴＣＰ／ＩＰで知られているＭＡＣアドレスをホスト識別情報として用いることが考えられる。ＭＡＣアドレスは、ビット数が比較的少なく、アクセス管理のために必要な記憶領域が少なくて済み、また物理的なネットワークインタフェースに固有の値であるので、詐称されにくい、という利点を持つ。
【００１２】
しかしながら、ＩＰネットワークにおいて、ルータを経由するとデータリンクフレームのＭＡＣアドレスはルータのネットワークカードのＭＡＣアドレスに書き換えられてしまう。従って、ホストとストレージ装置の間にルータがある場合、ターゲットはホストから受信したパケットからホストのＭＡＣアドレスを取得できないという問題がある。
【００１３】
上記特許文献１及び文献２には、ＩＰネットワークでＭＡＣアドレスをホスト識別のための情報として利用するに際して、ルータを経由する場合のＭＡＣアドレスを取得する方法についてまでは言及されていない。
【００１４】
本発明の目的は、iSCSIプロトコルを用いるストレージ装置に対するホストからのアクセス要求に関するセキュリティの向上を図ったアクセスの管理方法又はストレージ装置を提供することにある。
本発明の他の目的は、ＩＰネットワークに接続されたストレージ装置において、ＭＡＣアドレスを用いてホストを識別して、ホストからのログイン要求の許可の判定を行い得る方法又はストレージ装置を提供することにある。
本発明の他の目的は、ＩＰネットワークに接続されるストレージ装置に対するアクセスに関し、アクセス元のホストが同一のネットワークに属するか否かに応じて、ログイン要求処理やコマンドに関するアクセス管理の方法を変更することができるアクセスの管理方法を提供することにある。
【課題を解決するための手段】
【００１５】
本発明は、ＩＰネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、コマンドによって処理される対象となるデータを記憶する記憶装置と、ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、ホストコンピュータから送信されるログイン要求に関して、ログイン要求のフレームにホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定する第一判定手段と、第一判定手段による判定の結果、ログイン要求フレームに意図する第二の情報が含まれていない場合には、ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求する手段と、要求手段からの要求に対する応答として、ホストコンピュータから獲得した第一の情報に関して、アクセス管理テーブルを参照して判定する第二判定手段と、第二判定手段による判定の結果に応じて、ログイン要求の許可を行うものである。
好ましい例では、上記記憶装置は、iSCSIプロトコルによりアクセスさせる。また、上記アクセス管理テーブルに格納される第一の情報は、ホストコンピュータが接続されるＩＰネットワークのインタフェースのＭＡＣアドレスである。
【００１６】
本発明に係るアクセス管理方法は、外部の装置例えばホストコンピュータからネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理する

アクセス制御の管理方法において、外部から送信されるログイン要求のフレームをストレージ装置で受信するステップと、受信した該フレームに外部の装置を特定する第二の情報が含まれているかを判定する第一の判定ステップと、第一の判定の結果、フレームに第二の情報が含まれていない場合、外部の装置に対してそれを特定する第一の情報の取得を要求するステップと、取得された第一の情報に関してチェックを行い、アクセス許可をすべきかを判定する第二の判定ステップと、第二の判定の結果、許可された場合に外部の装置からストレージ装置に対するアクセス要求を許可するステップとを有する。

【００１７】

好ましい例において、ストレージ装置は、iSCSI層、ＴＣＰ層、ＩＰ層、データリンク層を有し、このストレージ装置をＩＰネットワークに接続される。
第一の情報として、好ましくはＭＡＣアドレスが使用され、第二の情報としてＩＰアドレスが使用される。
また、好ましくは、ストレージ装置へのアクセスが許可された外部装置を特定するＭＡＣアドレスを登録するテーブルが、ストレージ装置のメモリに予め用意される。そして、第二の判定ステップでは、外部装置から取得された第一の情報に関して、このテーブルを参照することにより判定が行なわれる。
また、第一の情報の取得を要求ステップにおいて、ＩＰネットワークに接続される装置を監視するためのＳＮＭＰマネージャにより外部の装置から第一の情報を送信するように要求する。

【００１８】

好ましい例では、ストレージ装置には、複数の論理装置（ＬＵ）が定義され、またアクセス管理テーブルには、ＭＡＣアドレスと、ＭＡＣアドレスのＩＰネットワークのインタフェースを持つ外部の装置がアクセス許可されたＬＵの識別符号が登録される。そして、前記第二の判定ステップの後に、外部の装置から送信されたコマンドの処理に関して、このテーブルを参照して予め登録されたＬＵに対するアクセスか否かを判定する第三の判定ステップを有し、この第三の判定の結果、許可されたＬＵに対してコマンドの処理が行なわれる。

【００１９】

本発明はまた、ネットワークに接続された第一の装置から第二の装置へのアクセスに関する許可を管理する方法、或いはコマンド処理の方法として把握される。この方法は、第一の装置から第二の装置に対するアクセスが同一のネットワーク間で行われるか否かを第一の装置から送信された情報のうちの第二の情報を用いてチェックする第一のチェックモードと、第一のチェックモードにおいて、同一のネットワーク間の通信でないと判定された場合、送信元となる第一の装置にから所定の第一の情報を獲得するステップと、獲得された第一の情報を用いて第二の装置へのアクセスの許可の可否をチェックする第二のチェックモードと、第二のチェックモードにおいて許可された場合に、第一の装置から第二の装置へ送信されるコマンドの処理を行う。

【発明の効果】

【００２０】

本発明によれば、ＩＰネットワークに接続されたiSCSIプロトコルを用いるストレージ装置において、ＭＡＣアドレスを用いてホストを識別して、ホストからのログイン要求の許可の判定が行える。
また、アクセス元のホストが同一のネットワーク（同一セグメント）に属するか否かに応じて、ログイン要求処理やコマンドに関するアクセス管理の方法を変更することができる。これにより、ストレージ装置に対するホストからのアクセス要求に関するセキュリティの向上が図れる。

【発明を実施するための最良の形態】

【００２１】

以下、図面を参照して本発明の実施形態を説明する。
図１は一実施形態によるデータ処理システムのハードウェア構成を示すブロック図である

。
このデータ処理システムは、IPネットワーク４００を介してホスト１００とストレージ装置２００が接続されて構成される。このネットワーク４００を介してホスト１００とストレージ装置２００の間でパケット形式のデータが送受信される。

【００２２】

ストレージ装置２００は、記憶制御装置２１０、複数のディスク装置２２０及びサービスプロセッサ（ＳＶＰ）２３０を備える。複数のディスク装置は、大量のデータを記憶する例えばＲＡＩＤ構成のディスクアレイ装置であり、ホストからのコマンド処理によりデータの書き込み読み出しが行われる。ＳＶＰ２３０は表示部及び入力部を備える。記憶制御装置２１０は、ホストアダプタ２４０、キャッシュメモリ２５０、ディスクアダプタ２６０、プロセッサ２７０、制御メモリ２８０を有する。ホストアダプタ２４０は、iSCSIポート２４２を有する。ポート２１１はギガビットイーサネットのような高速IPインタフェース４１０を介してIPネットワーク４００に接続される。

【００２３】

ホスト１００は、ＣＰＵ１１０、主記憶装置１２０、及び入出力処理装置１３０を有する計算機であり、具体的にはワークステーション、マイクロコンピュータ又はメインフレームコンピュータ等である。入出力処理装置１３０は、iSCSIポート１３２を有する。ポート１３２は高速IPインタフェース４１０を介してIPネットワーク４００に接続される。

【００２４】

尚、図示していないが、ホスト１００とストレージ装置２００は、ルータを介してＩＰネットワーク経由４００で接続される場合もある。また、接続する経路は一本であるとは限らない。

【００２５】

図２は、図１に示すデータ処理システムの論理的な構成を示す図である。
ホスト１００で生成されたコマンドまたはデータ５０は、iSCSI層９０AのiSCSIイニシエタ機能でプロトコル変換され、更にＴＣＰ層９２、ＩＰ層９４で制御情報（ヘッダ）を付加されてパケット処理され、データリンク層９６からネットワーク４００へ送信される。データリンク層はＭＡＣ（Media Access Control）層とも呼ばれ、例えばイーサネット（登録商標）やギガビットイーサネットとして実現される。

【００２６】

一方、ストレージ装置２００では、ネットワーク４００から受信されたコマンドまたはデータ５０は、データリンク層９６、ＩＰ層９４、ＴＣＰ層９２で処理され、各制御情報を除去される。そして、イニシエタのiSCSIイニシエタ機能が送り出した形でiSCSI層９０BのiSCSIターゲット機能へと送られ、処理される。各プロトコル処理層すなわちiSCSI層、ＴＣＰ層、ＩＰ層、データリンク層はハードウェアまたはプロセッサ上のソフトウェア、あるいはそれらの組み合わせにより実現される。
尚、ストレージ装置２００からホスト１００へデータが送信される時は、上記と逆のプロトコル処理が行われる。

【００２７】

本実施例で特徴的なことは、ホスト１００には、ＳＮＭＰエージェント９９Ａが実装され、ストレージ装置２００にＳＮＭＰマネージャ９９Ｂが実装される。そのために、ホスト１００とストレージ装置２００は、夫々ＵＤＰ層９８を持つ。また、ストレージ装置２００は、ホストを一意に識別する情報を格納するアクセス管理テーブル８０を有する。尚、アクセス管理テーブル８０の内容については図５を参照して後述する。

【００２８】

ここで、ＳＮＭＰ（Simple Network Management Protocol）の一般的な効用について概略説明しておきたい。
ＳＮＭＰは、IETF規格でRFC1157として定義された、ネットワークに接続された機器をネットワーク経由で監視するためのプロトコルであり、UDP/IP上で規定されて使用される。ＳＮＭＰは管理対象となる機器に常駐するＳＮＭＰエージェントと、管理する側の機器（

監視サーバ）上のＳＮＭＰマネージャ間で通信に用いられる。ＳＮＭＰマネージャとＳＮＭＰエージェントの間で行われる通信には３つの種類があるが、その内この実施例では、情報の要求と応答に関する通信の例を用いる。即ち、ＳＮＭＰマネージャからＳＮＭＰエージェントに、監視対象の機器の情報を要求し、一方、ＳＮＭＰエージェントは要求された情報を取得してＳＮＭＰマネージャに応答する。

【００２９】

ＳＮＭＰで管理される機器は、ＭＩＢ（Management Information Base）と呼ばれる機器の状態を表わすデータと、ＳＮＭＰマネージャの指示によりこれを操作するＳＮＭＰエージェントと呼ばれるプログラムを持つ。ＭＩＢとして定義されていればポート数など静的で変化の無い情報も、トラフィック状態など動的な情報もいずれも取得可能である。一般にＩＰネットワーク管理はネットワーク構成機器が多種・多数で困難な作業となりがちであるが、ＳＮＭＰとＭＩＢを利用することにより効率的な管理ができる。

【００３０】

ＳＮＭＰ処理やＵＤＰプロトコル処理に関しては、各プロトコル処理層すなわちiSCSI層、ＴＣＰ層、ＩＰ層、データリンク層の処理と同様にハードウェアまたはプロセッサ上のソフトウェア、あるいはそれらの組み合わせで実現される。例えばＳＮＭＰマネージャ９９ＢおよびＳＮＭＰエージェント９９Ａとしては、既に用意されているソフトウェアを用いても良い。例えばホスト１００のＯＳがLinuxならば、Linux 用に公開されているプログラムを入手してインストールして、適当にＭＩＢを設定する。

【００３１】

本実施例では、ＳＮＭＰマネージャ９９ＢはＭＡＣアドレスを獲得するために使用される。ＭＩＢ構造のなかでもＭＩＢ－２で定義されるＭＡＣアドレスの獲得にのみ特化したＳＮＭＰ機能を部分的にサポートしたソフトウェアとして実現する。この場合、ＳＮＭＰ機能はiSCSIターゲットおよびiSCSIイニシエタの機能の一部として実現できる。
アクセス要求を送信したホストを識別するために、ホストのポートのＭＡＣアドレスを用いる利点としては、ＭＡＣアドレスはビット数が少なくアクセス管理テーブルのために必要な記憶領域が少なくて済む。またＭＡＣアドレスはポートに固有の値であるので、詐称されにくいこと、が上げられる。

【００３２】

次に、ホスト１００のＳＮＭＰエージェントとストレージ装置２００ＳＮＭＰマネージャとの間の通信について簡単に説明する。（詳細は図６～８を参照して後述する。）
ホスト１００から送信されたiSCSIログイン要求Ｓ１を受信したストレージ装置のiSCSIターゲット機能９０Ｂは、ＳＮＭＰマネージャ９９Ｂに指示して、iSCSIログイン要求Ｓ１の発行元のネットワークアドレス（ＩＰアドレス）に対しＭＡＣアドレスを要求するために、ＳＮＭＰリクエストＳ２を送信させる。
ＳＮＭＰリクエストＳ２を受信したホスト１００のＳＮＭＰエージェント９９Ａは、通常のＳＮＭＰ処理として、要求されたＭＡＣアドレスを含むＭＩＢをＳＮＭＰレスポンスＳ３として応答する。このＳＮＭＰレスポンスＳ３を受信したＳＮＭＰマネージャ９９Ｂは、iSCSIターゲット機能９０Ｂへ受信したＭＡＣアドレスを報告する。

【００３３】

iSCSIターゲット機能９０Ｂは、獲得したホストのＭＡＣアドレスが、アクセス管理テーブル８０に登録されているか否かによりログインが正当であるか否かの判定を行なう。アクセス管理テーブル８０にそのＭＡＣアドレスが登録されている場合には、ログイン要求を許可し、それを伝えるためホストにログインレスポンスを返信する（Ｓ４）。
また、この様にしてログインが成立した後、ホストから受信するコマンドについて、予め許可されたＬＵへのアクセスか否かの判定を行ない、許可されたＬＵに対するコマンドの処理を行なう。尚、このアクセス制御処理の詳細については後述する。

【００３４】

図３は、iSCSIのイニシエタとターゲット間の通信に用いられるパケットのフォーマットの例を示す。

iSCSI層において、データの通信の単位となるＰＤＵ（iSCSI PDU）は、BHS（Basic Header Segment）３３とデータセグメント３４から構成される。ＢＨＳ３３とデータセグメント３４との間にＡＨＳ（Additional Header Sequence）が挿入される場合もあるが、図３の例ではそれを省略してある。

【００３５】

ＴＣＰ層、ＩＰ層、データリンク層では、iSCSI層からのパケットデータに対して先頭に、データリンクヘッダ（ＤＬＨ）３０、ＩＰヘッダ（ＩＰＨ）３１、ＴＣＰヘッダ（ＴＣＨ）３２が付加される。さらにiSCSIパケットデータの最後部にはデータリンクトレイラ（ＤＬＴ）３５が付加される。

【００３６】

ＩＰ層では、ＩＰアドレスと呼ぶ番号でノード（ネットワークに接続されている機器）の識別が行なわれる。現在広く普及しているIPv4では、ＩＰアドレスとして32ビットの数値が使われており、次世代のIPv6では128ビットの数値が用いられる。IPv4のIPヘッダでは先頭から13～16バイト目に発信元を示すソースＩＰアドレスが格納され、17～20バイト目に宛先を示すデスティネーションＩＰアドレスが格納される。

【００３７】

データリンク層において、各ネットワークカードには固有のアドレスが割り当てられ、このアドレスを基にしてデータリンクフレーム（データリンクヘッダから始まりデータリンクトレイラで終了する）の送受信が行なわれる。この固有のアドレスをＭＡＣアドレスと呼ぶ。ＭＡＣアドレスはイーサネットならば６バイト長であり、先頭の３バイトはベンダコードとしてIEEE（Institute of Electrical and Electronic Engineers ）が管理し割り当てを行なっている。残り３バイトは各ベンダで重複しないように管理しているコードである。このようにして設定されたＭＡＣアドレスは、他人のＭＡＣアドレスとは重複せず、全て異なるアドレスが割り当てられる。

【００３８】

データリンクヘッダの最初の６バイトは宛先を示すデスティネーションＭＡＣアドレスである。データリンクヘッダの次の６バイトは発信元を示すソースＭＡＣアドレスである。

【００３９】

図４に、ログイン要求フレームの構成例を示す。

ログイン要求或いはログインレスポンスのフレームは、基本的に似ている。図４は、ログイン要求、ログインレスポンスフレームの、主にiSCSIのＰＤＵの部分を示す。いずれのフレームも１ワードが４バイトずつで、ＢＨＳは４８ワードから構成されている。

【００４０】

ＢＨＳの後にはデータセグメントが付加される。ログイン要求フレームおよびログインレスポンスフレームでは、データセグメントにiSCSI通信に必要な各種パラメータを格納して、それらの交換やネゴシエーションを行う。パラメータは、ＴＥＸＴ形式と呼ぶ、<キー>=<値>　で表される形式で記述される。データセグメントは可変長（４バイトの倍数）である。

【００４１】

ログインレスポンスのステータス領域（Status-ClassとStatus-Detailを合せた領域）にはログインのステータスが格納される。ステータスが０００００（Status-Class及びStatus-Detailが００）ならば、ログインが成功している状態を示す。ステータスが０００００以外ならば何らかの理由でログインが成功していない状態を示し、イニシエタは別のパラメータでログインを試みるか、或いはログインをあきらめる。

【００４２】

次に、図５を参照してアクセス管理テーブル８０について説明する。

アクセス管理テーブル８０には、各行ごとにホストのネットワークインタフェースのＭＡＣアドレス81と、それに対応するＩＰアドレス82と、ＭＡＣアドレスを持つホストに対しアクセス許可するＬＵのリスト83と、ＭＡＣアドレスを持つホストとの通信状況(Session

)84が登録される。

【００４３】

通信状況84は、例えば次の様に表される。

（１）iSCSIログイン要求受信前であってホストとの通信が行なわれていない（"not establish"）

（２）iSCSIログイン要求を受信して判定中であり、iSCSIログインレスポンスを応答してログイン成立前（"login"）

（３）iSCSIログイン成立後("establish")

アクセス管理テーブル８０は、ホストとアクセスを許されたＬＵをアクセス管理テーブルに設定するために、それらの内容をコンソールＳＶＰ２３０の表示部に表示したり、その入力部からの操作により登録内容の変更が可能である。

【００４４】

次に図６～図８のフローチャートを参照して、アクセス制御処理の詳細について説明する。

ストレージ装置１００は、ホスト１００から送信されたiSCSI Login 要求Ｓ１を受信すると（１１００）、そのiSCSI Login 要求Ｓ１のＩＰヘッダを参照して、ソースアドレスが自ポートと同一セグメント内のＩＰアドレスであるか否かを判定する（１１１０）。

この判定の結果、iSCSI Login 要求Ｓ１のソースＩＰアドレスが自ポートと同一ネットワーク内で無かった場合、同一ネットワーク外のポートからログイン要求があったことを制御メモリ２８０内のログに記録する（１１２０）。そしてＳＮＭＰマネージャ９９Ｂに、iSCSI Login 要求フレームのソースＩＰアドレスに対するＭＩＢ獲得を指示する（１１３０）。この指示に従って、ＳＮＭＰマネージャ９９Ｂは、ＳＮＭＰリクエストＳ２をホストへ送信する。

【００４５】

次に、ホスト１００でＳＮＭＰリクエストが拒絶されたか又はＳＮＭＰレスポンスがホストから応答されず一定時間経過した（タイムアウトが発生した）か否かが判定される（１１４０）。もしＳＮＭＰリクエストＳ２に対するＳＮＭＰレスポンスＳ３が、タイムアウトを起こさずにストレージ装置２００で受信できた場合、そのＳＮＭＰレスポンスで獲得したホストのポートのＭＡＣアドレスが、アクセス管理テーブル８０に登録されているか否かが判定される（１１５０）。その判定の結果、テーブル８０に登録されている場合には、ホスト１００からのアクセスが許可されているため、ログインを許可するiSCSI Login レスポンスＳ４をホストに対して返信する（１１６０）。

【００４６】

この後は、図６に示すiSCSI の Full Feature phase に移る（１４００）。この場合、ログイン要求をしてきたホスト１００はストレージ装置２００とは異なるセグメントにあるので、ホスト１００から送信された各フレームのＭＡＣアドレスは途中のルータ装置で書き換えられるため、ホスト識別情報としては、ホスト送信フレームのソースＩＰアドレスを用いる。

【００４７】

ホスト１００からCommand PDUを受信したら（１４１０）、アクセス管理テーブル８０を参照して、コマンドが格納されたフレームのソースＩＰアドレスについて、そのコマンドが示すＬＵが登録されているか否かを判定する（１４２０）。この判定の結果、もしＬＵが登録されていれば、そのＬＵへのアクセス許可が有ると判断して、そのＬＵに対してコマンドの処理を行ない（１４３０）、そのコマンドの処理を終了する（１４４０）。

【００４８】

一方、ステップ１４２０の判定において、ソースＩＰアドレスから、もしコマンドが示すＬＵが登録されていなければ、そのＬＵへのアクセスが許可されていないアクセス要求があったことをログに記録し（１４５０）、そのコマンドの処理を行なわずに終了する。

【００４９】

さて話を戻して、上記ステップ１１１０の判定の結果、「Ｙｅｓ」であるときには、図

７に示す処理が行なわれる。この場合、ログイン要求をしてきたホスト１００はストレージ装置２００と同一セグメントにあるので、ホストから送信された各フレームのソースＭＡＣアドレスをホスト識別情報として利用できる。

【００５０】

まず、iSCSI Login リクエストＳ１のソースＭＡＣアドレスがアクセス管理テーブル８０に登録されているか否かを判定する（１２３０）。この判定の結果、もしテーブル８０に登録されていれば、ホスト１００からのアクセスが許可されているので、ログインを許可する旨のiSCSI Login レスポンスＳ４をホストへ返信する（１２４０）。この後、iSCSI の Full Feature phase となる（１３００）。すなわちホスト１００からCommand PDUを受信したら（１３１０）、アクセス管理テーブル８０を参照して、そのコマンドが格納されたフレームのソースＭＡＣアドレスに関し、コマンドが示すＬＵが登録されているか否かを判定する（１３２０）。もしＬＵが登録されていれば、そのＬＵに関してコマンドの処理を行ない（１３３０）、そのコマンドの処理を終了する（１３４０）。

【００５１】

一方、上記ステップ１３２０の判定で、ソースＭＡＣアドレスから、そのコマンドが示すＬＵが登録されていない場合は、そのＬＵへのアクセスが許可されていないアクセス要求があったことをログに記録し（１３５０）、そのコマンドの処理を行なわずに終了する。

【００５２】

また、上記ステップ１２３０の判定の結果「Ｎｏ」であった場合、またはステップ１１４０の判定の結果「Ｙｅｓ」であった場合、またはステップ１１５０の判定の結果「Ｎｏ」であった場合には、ログインを許可しない旨のiSCSI Login レスポンスをホスト１００へ応答（ステータスとして０００００以外を応答）する（１２００）。すなわちこの場合には、ＭＡＣアドレスを用いてホストを識別できなかった、或いはホストのＭＡＣアドレスがアクセス管理テーブル８０に登録されていなかったので、アクセスを許可されていないポートからのログイン要求が有ったものと判断する。そして未登録のポートからログイン要求があったことをログに記録して終了する（１２１０）。

【００５３】

尚、上記ログに関して言えば、ログとして相手ポートのＩＰアドレス及びイベントの発生時刻がイベント毎に取得されて、制御メモリ２８０に記憶される。この様に取得されたログは、その後管理者の操作又は予め定められたスケジュールに従ってＳＶＰ２３０の表示部に表示される。管理者はその表示内容から判断して、ネットワークの切り離しや、及び目的外のホストからのアクセスの防止のための操作を行える。

【００５４】

以上、一実施形態について説明したが、以下種々の変形例について説明する。

上記実施形態では、ステップ１１１０でiSCSI Login リクエストＳ１を送信したポートが自ポートと同一セグメントに属するか否かを iSCSI Login リクエストが格納されたＩＰパケットのソースＩＰアドレスで判定している。しかしながら変形例では、そのソースＩＰアドレスに代わって、ＩＰパケットがカプセル化されたイーサネットフレームのフレームヘッダに含まれるソースＭＡＣアドレスで判定しても良い。すなわち、ソースＭＡＣアドレスが、ルータのポートのＭＡＣアドレスである場合、イーサネットフレームはルータを経由して自ポートに到達したので、iSCSI Login リクエストを発行したポートは同一ネットワークに属さない。ソースＭＡＣアドレスが、ルータのポートのＭＡＣアドレスでない場合、イーサネットフレームはルータを経由せず自ポートに到達したので、iSCSI Login リクエストを発行したポートは同一ネットワークに属する。

判定の結果、分岐した後の処理（ステップ１１２０以降またはステップ１２３０以降の処理）は、前述の通りである。

【００５５】

また他の変形例について言えば、上記実施形態では、ログイン成立後も受信した各コマンドに関して、それを送信したホストをＭＡＣアドレスまたはＩＰアドレスを基に識別し

て、ＬＵへのアクセス可否を判定している。これに対して変形例では、処理の簡略化または高速化などの要望に応えるために、単にログイン要求フレームの受信時に未登録のホストからのログインを拒否するだけならば、図６のステップ１４２０、及び又は図７のステップ１３２０の判定を省略し、full feature phase開始後は、受信したPDUを全てチェックせずに処理を行なうこともできる。
この場合、アクセス管理テーブル８０には、単にログインを許可するホストのＭＡＣアドレスのみを登録しておけば良い。例えば図９に示すようにＭＡＣアドレスのリスト形式の登録テーブルとすれば良い。

【００５６】

更に他の変形例において、full feature phase(１３００又は１４００)で、全ての各コマンドに関して、それらを送信したホストをＭＡＣアドレスまたはＩＰアドレスを基に識別し、ＬＵへのアクセス可否の判定は行わず、例えばストレージ装置２００への書き込み（write）を指示するコマンドに関してのみホストのアクセス可否の判定を行ない、それ以外のコマンドはその判定を行わず処理することも可能である。

【００５７】

更に他の変形例において、ログアウトした後も、前回のログイン時の情報（ホストのＭＡＣアドレス、IPアドレス）をアクセス管理テーブルに記憶しておいて、次回のログイン時の認証に利用することも可能である。

【００５８】

更に他の変形例に関して、図２を参照した上記実施形態では、ホストとストレージ装置との間のデータの通信を前提としていた。しかし、変形した例では、ストレージ装置どうしでデータ通信する場合にも適用できる。この場合、片方のストレージ装置がホストの役割を果たす。すなわちホストの役割を果たす側のストレージ装置の記憶制御装置２１０が持つプロセッサ２７０、またはホストアダプタ２４０が持つプロトコル処理用ハードウェア、あるいはそれらの組み合わせでホストとしてのプロトコル処理を実現する。

【００５９】

また他の例として、１つ又は複数のストレージ装置２００にＩＰインタフェースを介して接続する管理サーバを設け、この管理サーバに図１示すＳＶＰ２３０に加え又はそれに代わって上記ＳＶＰ２３０の機能、例えばログの記録等の処理を行わせても良い。この管理サーバにより複数のストレージ装置を一元的に監視することが可能となる。

【００６０】

更にまた上記実施形態では、ストレージ装置からホストのＭＡＣアドレスを獲得するためにＳＮＭＰリクエストを用いたが、別の手段を用いることもできる。例えば、iSCSIのTEXT Mode negotiation と呼ぶ、イニシエタとターゲット間で各種動作パラメータの交換をするためのプロトコルを用いて、イニシエタに対しＭＡＣアドレスを送信するように要求することができる。
その場合、ＳＮＭＰマネージャやＳＮＭＰエージェントをストレージ装置やホストが持つ必要は無いが、ホストはTEXT Requestで示されたＭＡＣアドレス要求を理解し、TEXT ResponseとしてＭＡＣアドレスを応答する機能を持つ必要がある。TEXT Request及びTEXT Responseは、各々ＴＥＸＴ形式で記述される。

【００６１】

図１０に、iSCSIのTEXT Mode negotiationによるＭＡＣアドレスの獲得のためのアクセス制御処理の一例を示す。

【００６２】

イニシエタからターゲットに対してiSCSI Login リクエストが発せられると（Ｓ１）、ターゲットからイニシエタには、iSCSI Login レスポンスが返される。この例では、ＭＡＣアドレスに基くセキュリティを利用する旨の問合せ用として、ベンダが独自に設定したＸで始まるキー「X-com.・・security」をデータセグメントに用いて返信する（Ｓ２）。このようにターゲットが新しいパラメータを示したので、これに対してイニシエタは、ログインフェーズを続ける。この例では、イニシエタが、「X-com.・・security」と言うキ

ーを知っていて、「ＭＡＣアドレスに基くセキュリティを利用する」ことに同意している。そこで、イニシエタは、ターゲットとの通信に用いるポートのＭＡＣアドレス「0123456789AB」をターゲットへ送信する（Ｓ３）。それを受信したターゲットは、「0123456789AB」が管理テーブルに予め設定したあったＭＡＣアドレスであったので、ログインを許可する。反対に、もし登録されていないＭＡＣアドレスならば、００００以外のステータスを応答してログインを拒否する（Ｓ４）。

【００６３】

次に、ログインの失敗した場合（Ｂ）について説明する。

ISCSI規格では、TEXT Mode negotiationにて知らないキーに対しては、イニシエタはターゲットに対して、「Not Under Stood」の値を応答する（Ｓ３）ように規定されている。それを受信すると、ターゲットはＭＡＣアドレスを獲得できないので、ログインを許可しない（Ｓ４）。

このように、iSCSIのTEXT Mode negotiationを使用してＭＡＣアドレスを獲得できる。

【００６４】

以上、いくつかの実施例について説明したが、本発明は上記実施例に限定されるものでなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。

【図面の簡単な説明】

【００６５】

【図１】一実施形態におけるデータ処理システムのハードウェア構成を示すブロック図。

【図２】一実施形態によるデータ処理システムにおけるiSCSIのイニシエタとターゲット間の通信の概念を示す図。

【図３】iSCSIのイニシエタとターゲット間の通信に用いられるパケットのフォーマットの例を示す図。

【図４】ログイン要求フレームの構成例を示す図。

【図５】図１に示すアクセス管理テーブル８０構成例を示す図。

【図６】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図７】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図８】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図９】他の実施形態によるアクセス管理テーブルの他の例を示す図。

【図１０】ＭＡＣアドレスの獲得ための他の実施形態によるアクセス制御処理のシーケンスを示す図。

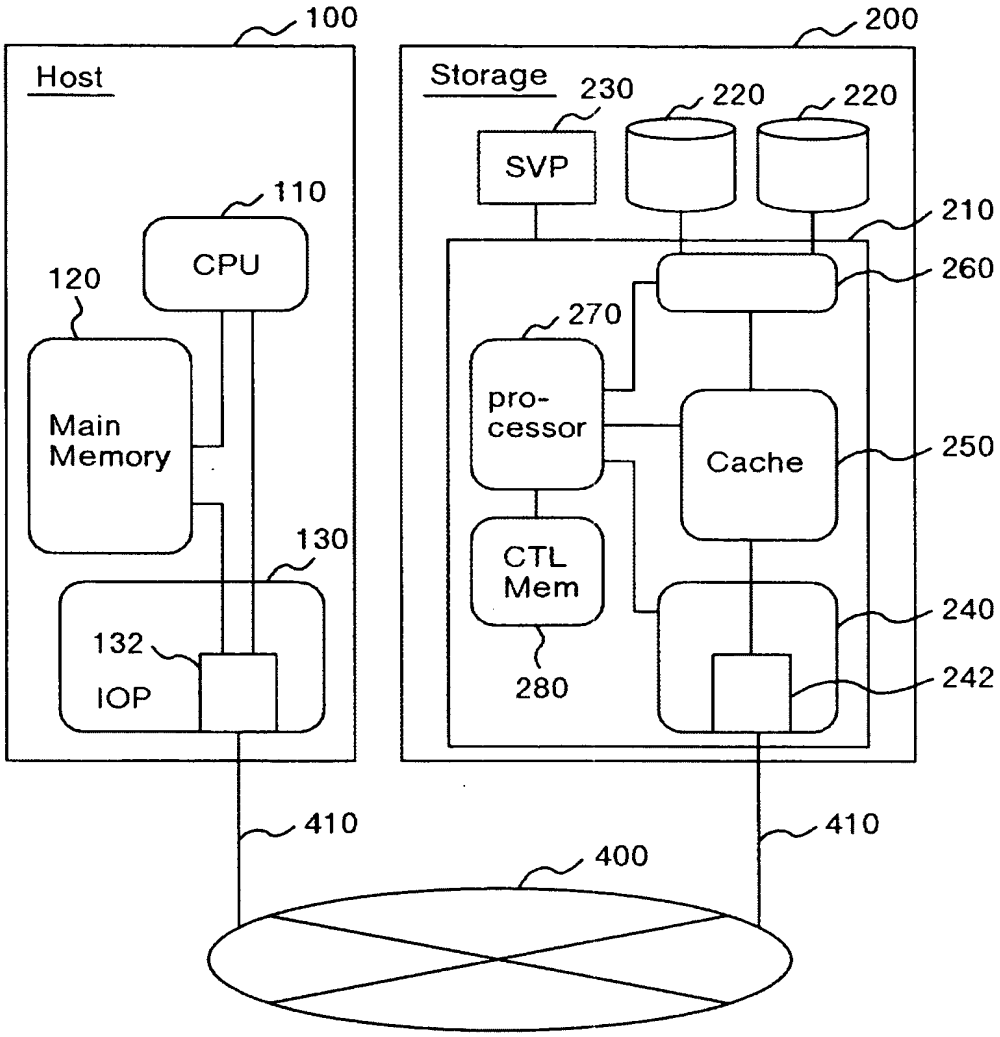
【符号の説明】

【００６６】

100：ホストコンピュータ、　200：ストレージ装置
400：ＩＰネットワーク、　410：高速ＩＰインタフェース
10：ログイン要求フレーム、　20：ＳＮＭＰ要求フレーム
30：ＳＮＭＰ応答フレーム、　40：ログイン応答/拒絶フレーム
80：アクセス管理テーブル、
90A：iSCSI層（イニシエタ）、　90B：iSCSI層（ターゲット）
92：ＴＣＰ層、　94：ＩＰ層
96：ＭＡＣ層、　98：ＵＤＰ層
99A：ＳＮＭＰエージェント、　99B：ＳＮＭＰマネージャ

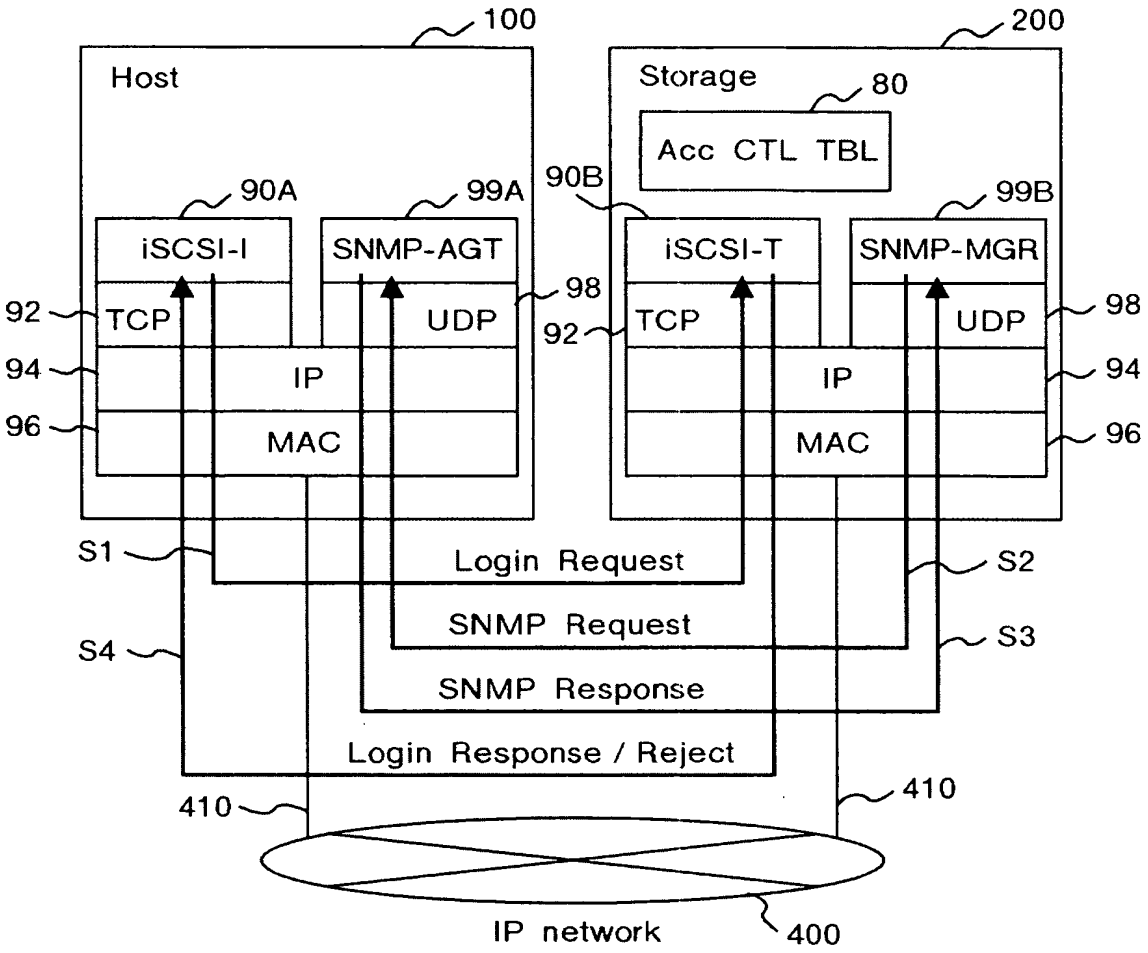
【書類名】図面
【図１】

図　1


100
Host
110
CPU
120
Main
Memory
130
132
IOP
200
Storage
230
SVP
220
220
210
260
270
pro-
cessor
Cache
250
CTL
Mem
280
240
242
410
410
400

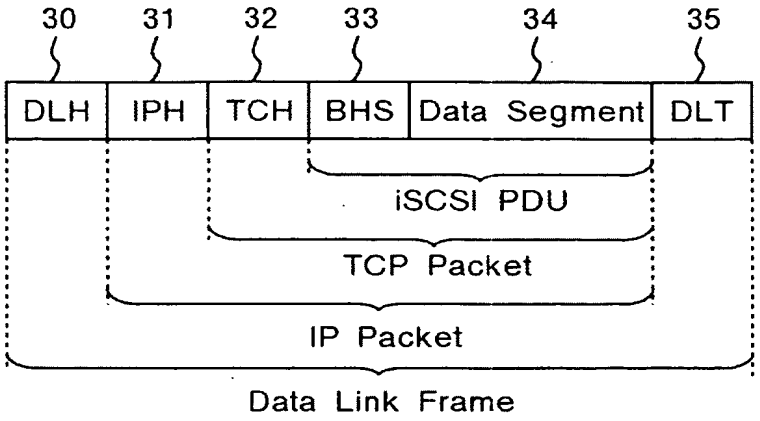
【図２】

図　2


100
Host
200
Storage
80
Acc CTL TBL
90A
99A
90B
99B
iSCSI-I
SNMP-AGT
iSCSI-T
SNMP-MGR
92
TCP
UDP
98
94
IP
96
MAC
S1
Login Request
S2
SNMP Request
S4
S3
SNMP Response
Login Response / Reject
410
410
IP network
400

【図３】

図　3

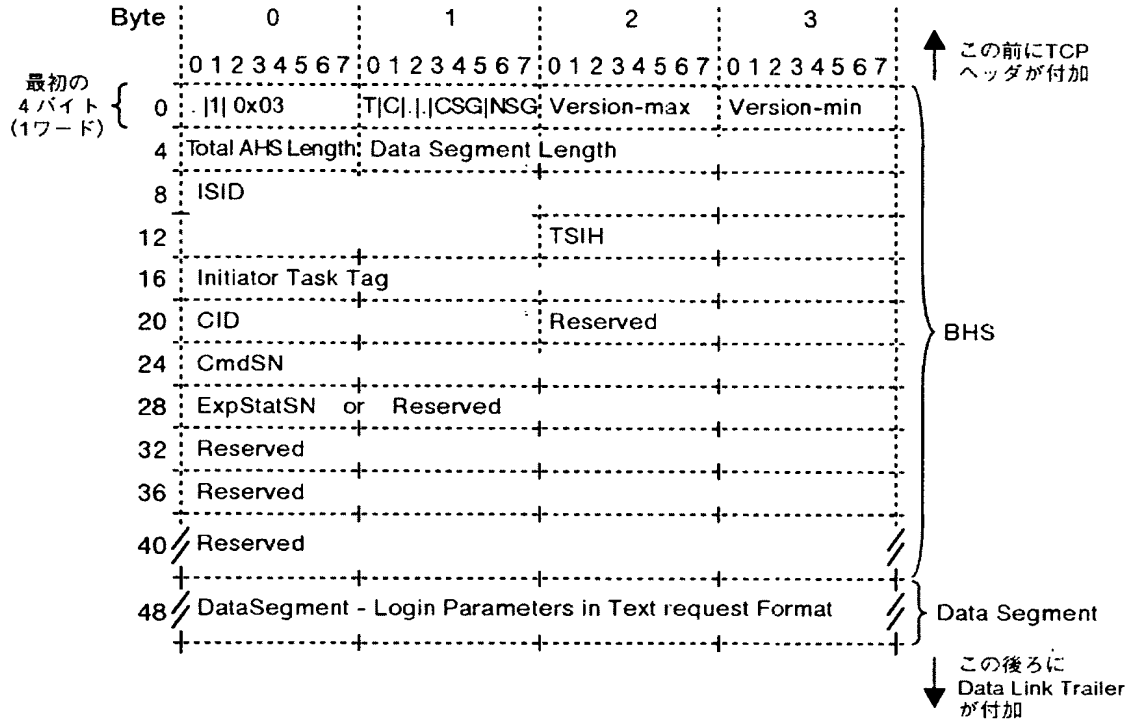


DLH : Data Link Header
IPH : IP Header
TCH : TCP Header
BHS : Basic Header Segment
DLT : Data Link Trailer

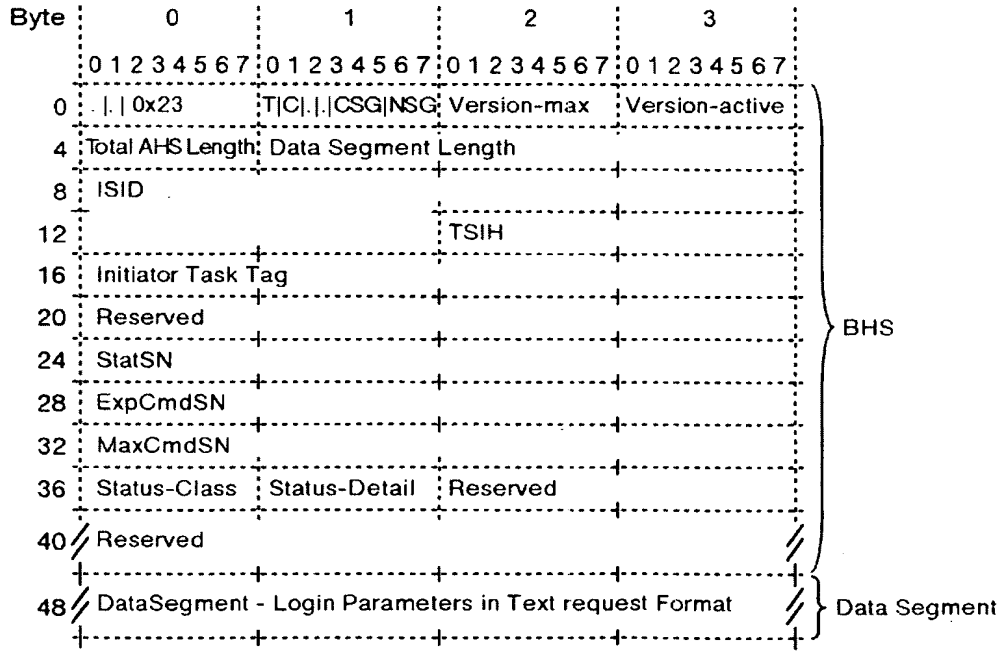
【図４】

図　4

（A）ログイン要求 (Login Request)

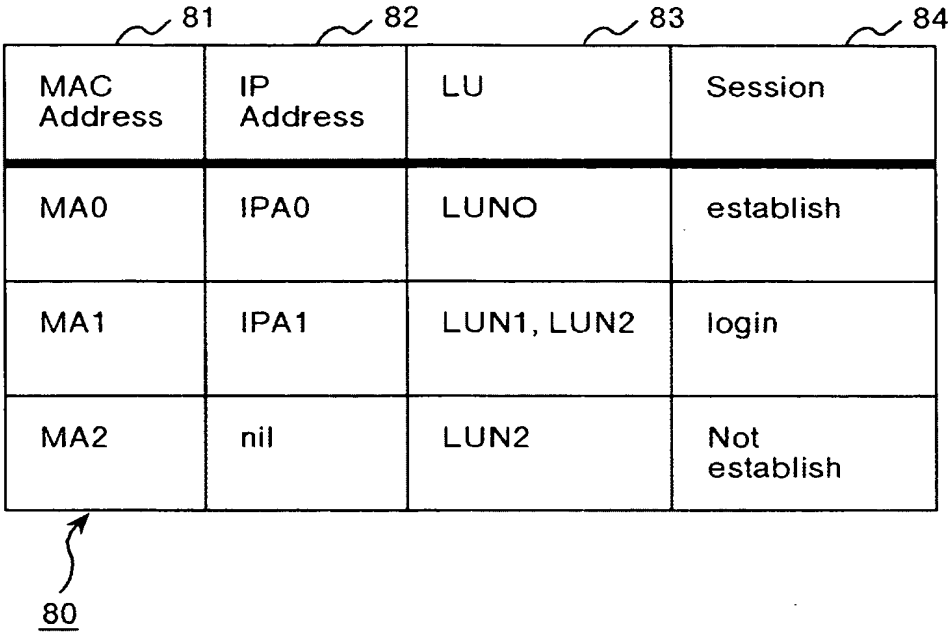


（B）ログインレスポンス (Login Response)



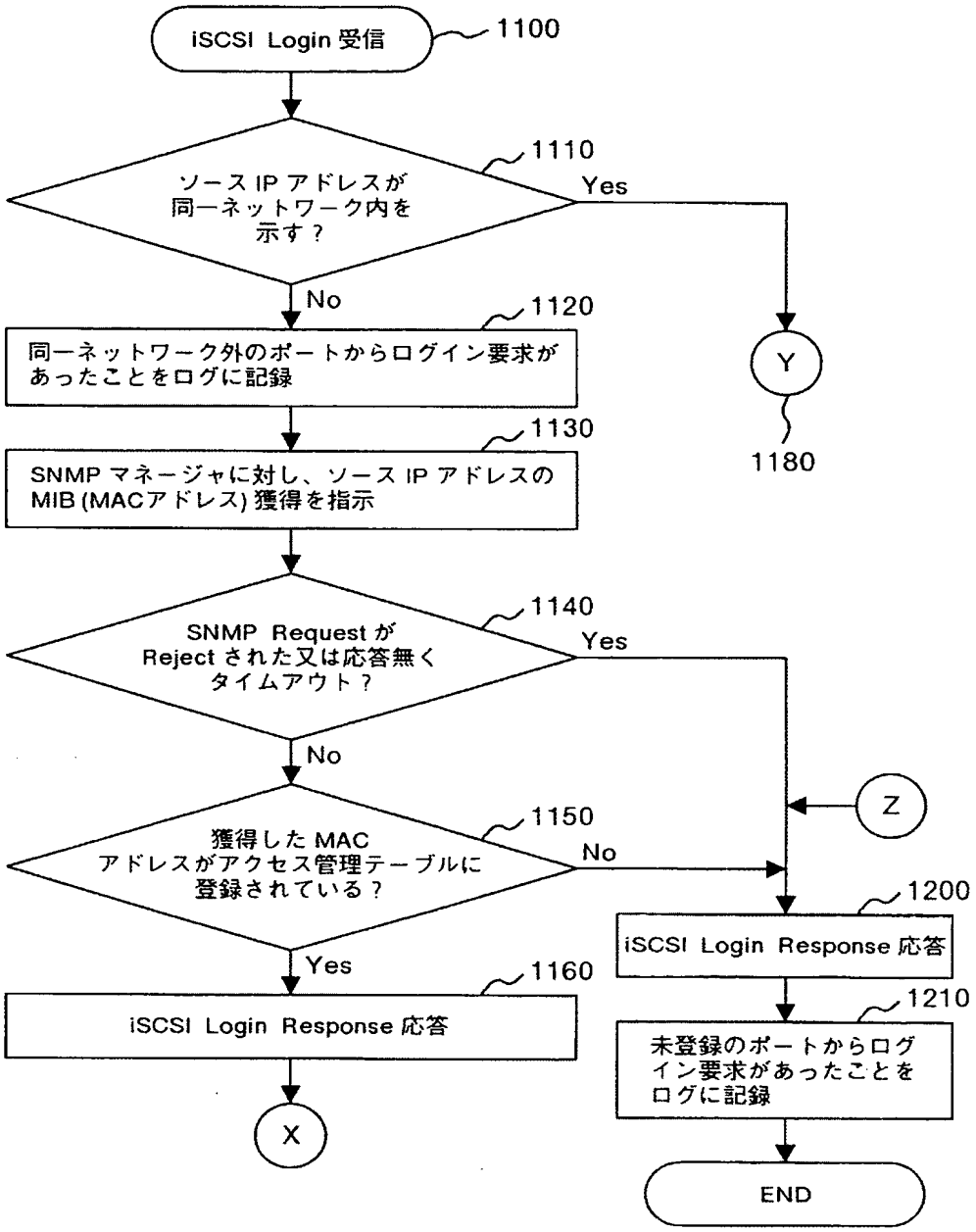
【図５】

図　5


81
82
83
84
MAC Address
IP Address
LU
Session
MA0
IPA0
LUNO
establish
MA1
IPA1
LUN1, LUN2
login
MA2
nil
LUN2
Not establish
80

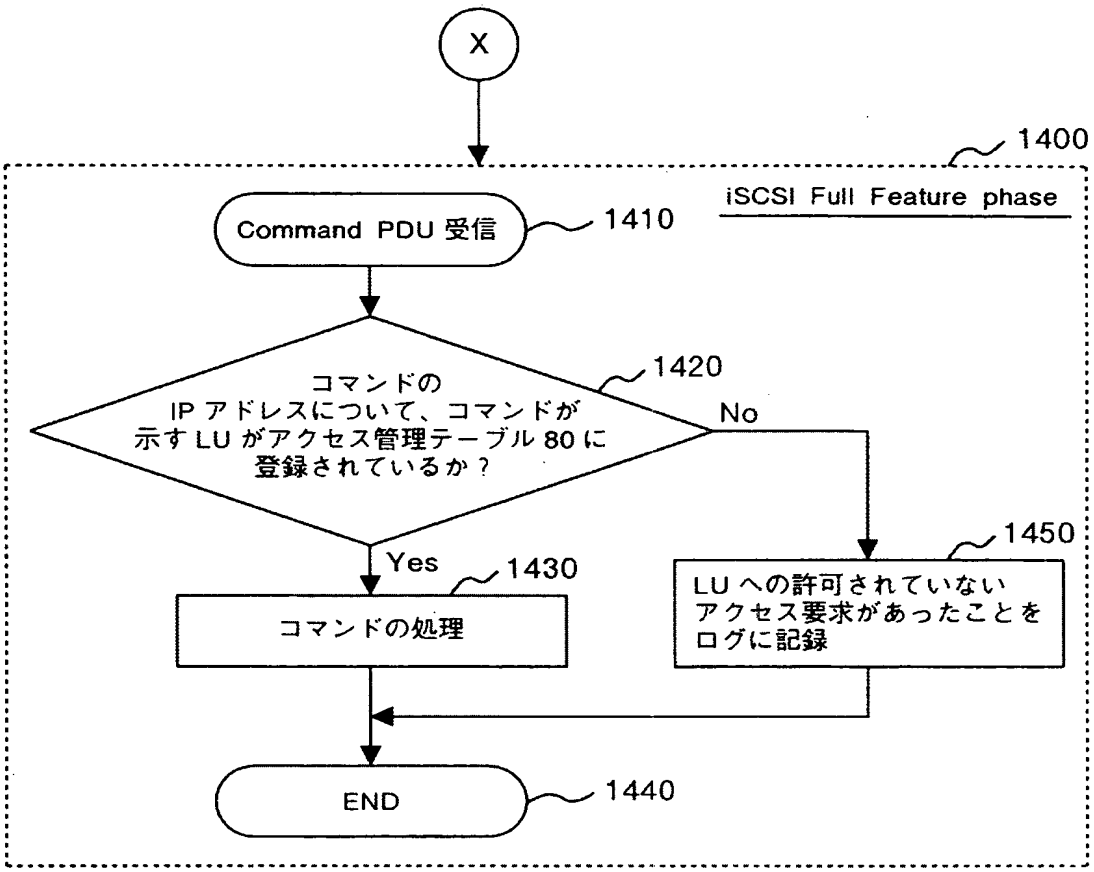
【図６】

図　6


iSCSI Login 受信
1100
ソース IP アドレスが同一ネットワーク内を示す？
1110
Yes
No
同一ネットワーク外のポートからログイン要求があったことをログに記録
1120
Y
1180
SNMP マネージャに対し、ソース IP アドレスの MIB (MACアドレス) 獲得を指示
1130
SNMP Request が Reject された又は応答無くタイムアウト？
1140
Yes
No
Z
獲得した MAC アドレスがアクセス管理テーブルに登録されている？
1150
No
Yes
1200
iSCSI Login Response 応答
1160
iSCSI Login Response 応答
1210
未登録のポートからログイン要求があったことをログに記録
X
END

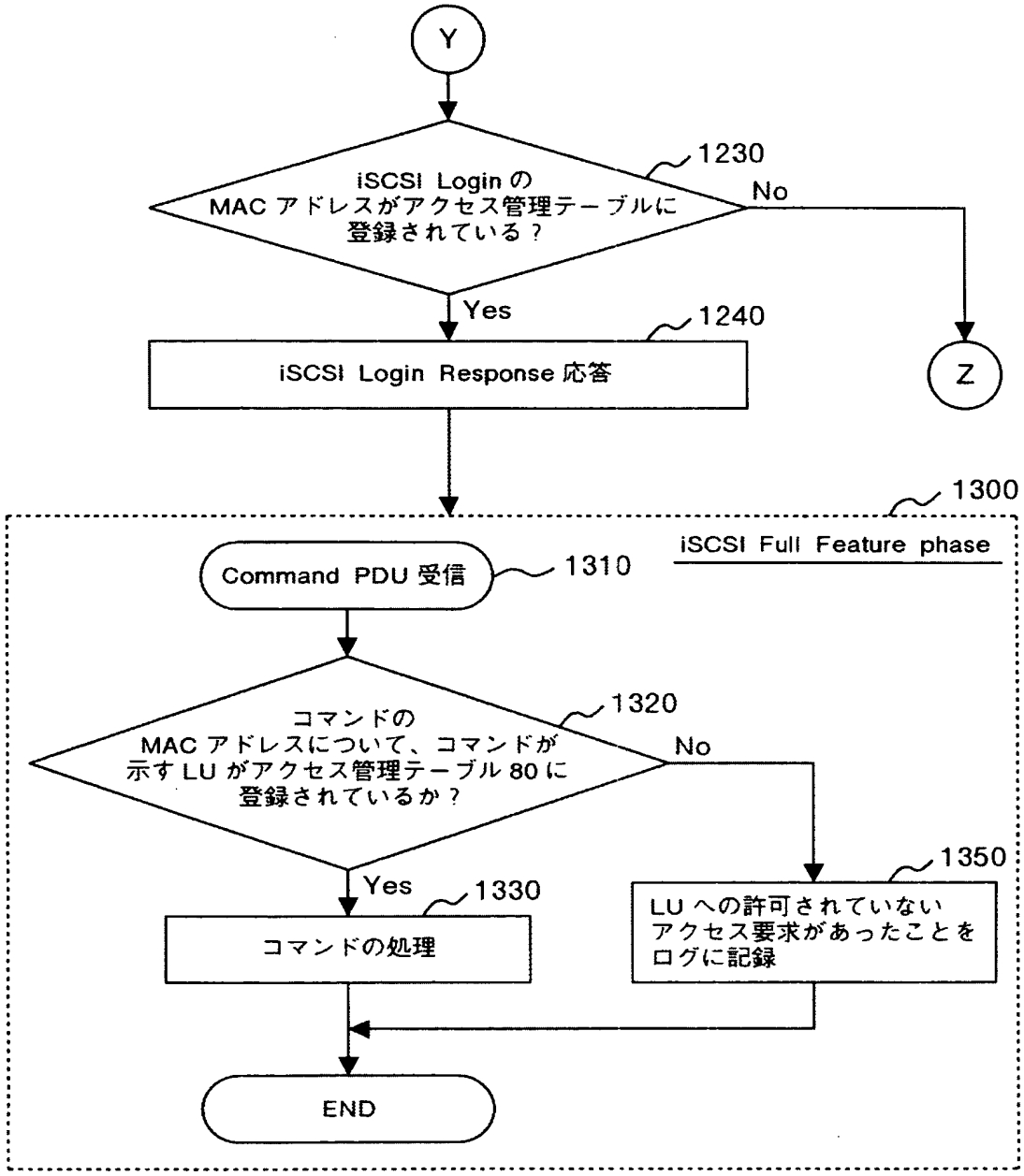
【図７】

図　7


X
1400
iSCSI Full Feature phase
Command PDU 受信
1410
コマンドの
IP アドレスについて、コマンドが
示す LU がアクセス管理テーブル 80 に
登録されているか？
1420
No
Yes
1430
コマンドの処理
1450
LU への許可されていない
アクセス要求があったことを
ログに記録
END
1440

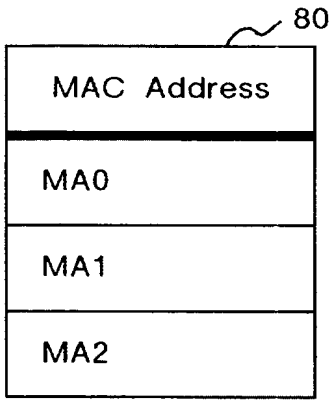
【図８】

図　8


Y
1230
iSCSI Login の
MAC アドレスがアクセス管理テーブルに
登録されている？
No
Yes
1240
iSCSI Login Response 応答
Z
1300
iSCSI Full Feature phase
Command PDU 受信
1310
コマンドの
MAC アドレスについて、コマンドが
示す LU がアクセス管理テーブル 80 に
登録されているか？
1320
No
1350
LU への許可されていない
アクセス要求があったことを
ログに記録
Yes
1330
コマンドの処理
END

【図９】

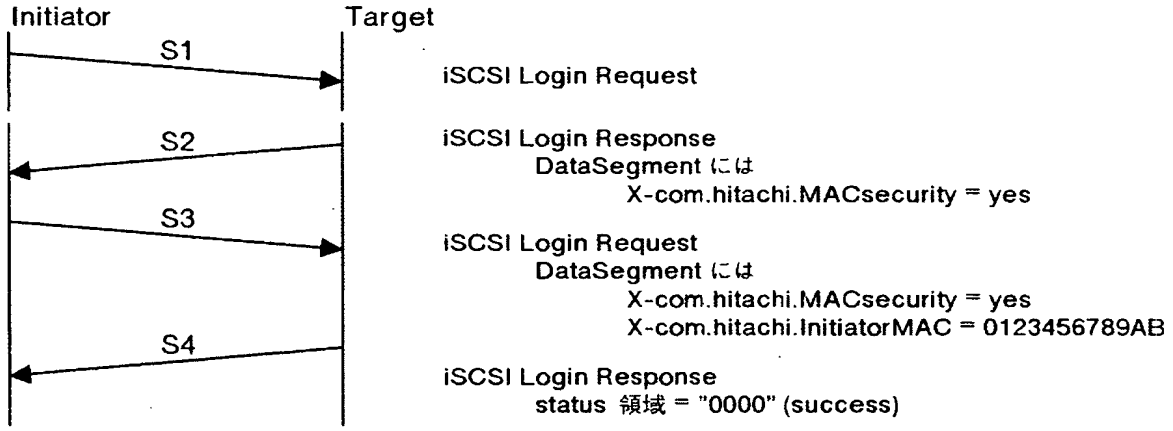
図　9



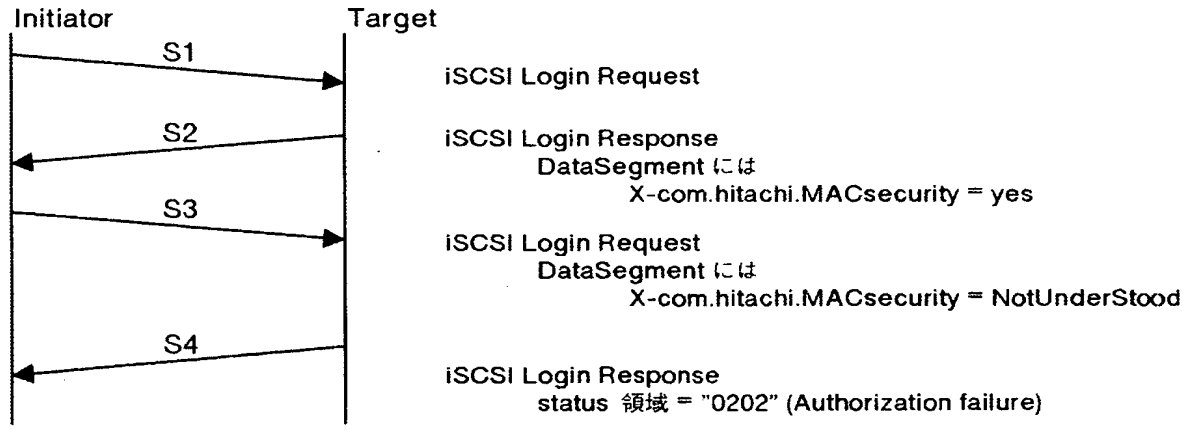
【図１０】

図　１０

（Ａ）ログイン許可の場合



（Ｂ）ログイン失敗の場合



【書類名】要約書
【要約】
【課題】
iSCSIプロトコルを用いるストレージ装置へのホストからのアクセス要求に対するセキュリティの向上を図る。
【解決手段】
外部の装置からネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理するアクセス制御の管理方法において、外部から送信されるログイン要求のフレームをストレージ装置で受信し、受信した該フレームに外部の装置を特定する第二の情報が含まれているかを判定し（第一の判定）、第一の判定の結果、そのフレームに第二の情報が含まれていない場合、外部の装置に対してそれを特定する第一の情報の取得を要求し、取得された第一の情報に関してチェックを行い、アクセス許可をすべきかを判定し（第二の判定）し、第二の判定の結果、許可された場合に外部の装置からストレージ装置に対するアクセス要求を許可する。
【選択図】　図２

特願２００３－３６７１５２

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所